區網會議

李墨軒

112.07.05.

資安通報

教育機構資安通報平台

- https://info.cert.tanet.edu.tw/prog/index.php
  - 更新聯絡人資訊
  - 定期修改密碼
  - 填寫資安長資訊

填寫/修改資安長資訊


教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
機關名稱:國立臺灣大學
使用者:李墨軒
主管機關:臺北區域網路中心(1)
聯絡電話:02-3366-5012#
E-Mail:molee@ntu.edu.tw
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw
回首頁
修改個人資料
修改資安長資料
登出
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
尚有8173張EWA預警單未處理，請按此查閱相關資訊

通報應變

- 通報時間1hr
- 自行通報應變
- 申請DDOS

通報時間

事件單編號	單位名稱	發佈時間	距通報時間	流程
203374	[redacted]	2022-12-12 08:15:23	29	新進工單

- 通報時間1hr
  - 可至事件單查看

資安通報時間查詢


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
情資資料下載
事件統計
開始日期:
結束日期
查詢
資安事件數
平均通報處理時間
平均應變處理時間
平均全部處理時間
1617
00:15:29
00:00:00
00:15:29
Page 1/1

Mo

弱掃平台

https://evs.ncku.edu.tw/

弱掃平台

- 弱掃平台網址
  - https://evs.ncku.edu.tw/
- 各校有一組帳密
- 可自行申請掃描
- 沒有帳密可向區網中心詢問，區網中心可協助重置

中高風險網站

單位	網站	最新檢測						
	網站網址 | 網站名稱 | 建立時間 | 重要程度	排程日期 ▼	狀態	風險				
				高風險	中風險	低風險	信　息	
國立臺灣大學	2022-1 普通	2022-12-12 00:00	執行完成	0	0	6	5	修改 | 檢測記錄
國立臺灣大學	2022-1 普通	2022-11-25 00:00	執行完成	0	0	1	5	修改 | 檢測記錄
國立臺灣大學	教務處 2019-1 普通	2022-11-17 00:00	執行完成	1	6	6	8	修改 | 檢測記錄

OWASP Top 10

OWASP Top 10

Open Web Application Security Project

https://owasp.org/www-project-top-ten/

https://owasp.org/Top10/zh_TW/

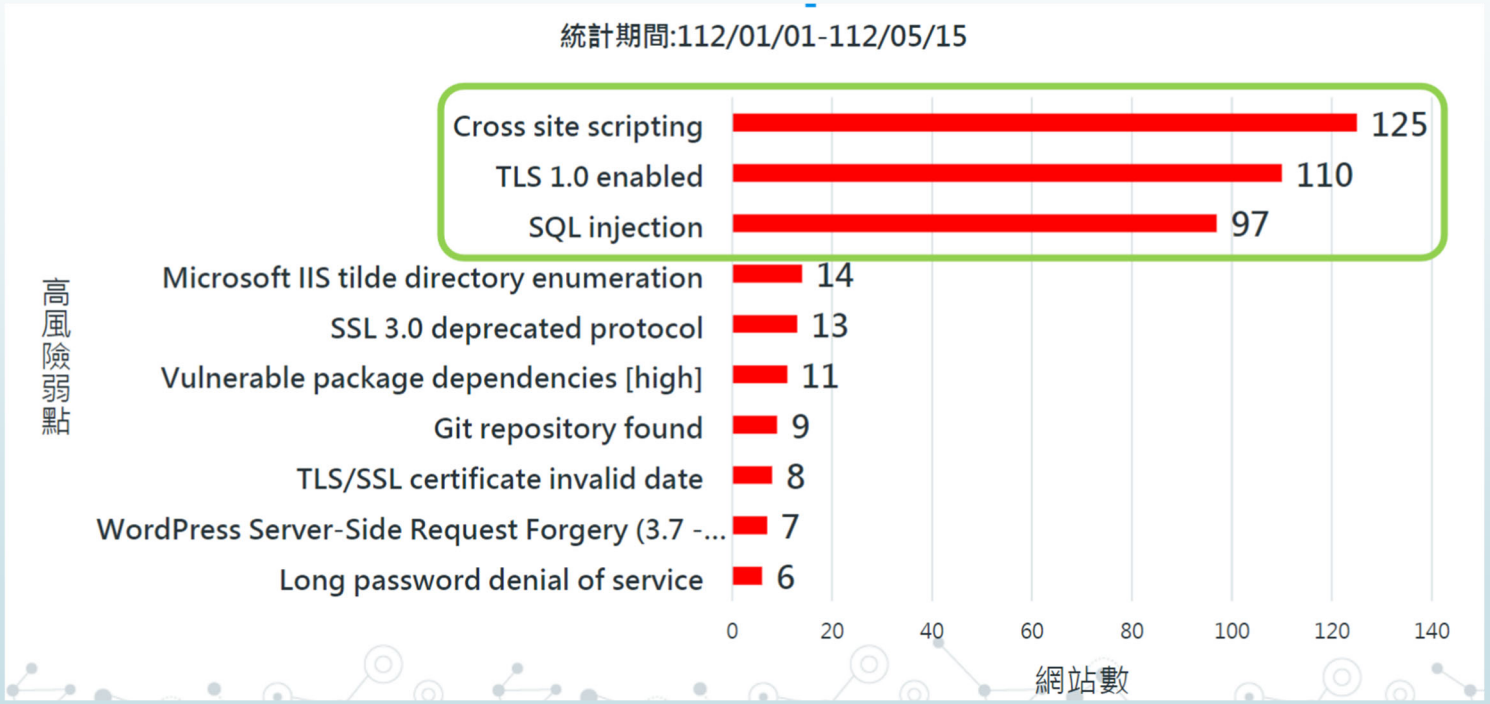
常見網站應用程式弱點 Top 10 (2017)

A1 Injection 注入攻擊
A2 Broken Authentication 無效身分認證
A3 Sensitive Data Exposure 敏感資料外洩
A4 XML External Entity, XML 外部處理器漏洞
A5 Broken Access Control 無效的存取控管
A6 Security Misconfiguration 不安全的組態設定
A7 XSS (Cross-Site Scripting) 跨站攻擊
A8 Insecure Deserialization 不安全的反序列化漏洞
A9 Using Components with Known Vulnerabilities使用已有漏洞的元件
A10 Insufficient Logging & Monitoring 紀錄與監控不足風險

常見網站應用程式弱點 Top 10 (2021)

A1 Broken Access Control 無效的存取控管
A2 Cryptographic Failures 加密機制失效
A3 Injection 注入攻擊
A4 Insecure Design 不安全的設計
A5 Security Misconfiguration 不安全的組態設定
A6 Vulnerable and Outdated Components 危險或過舊的元件
A7 Identification and Authentication Failures 認證及驗證機制失效
A8 Software and Data Integrity Failures 軟體及資料完整性失效
A9 Security Logging and Monitoring Failures 資安記錄及監控失效
A10 Server-Side Request Forgery(SSRF) 伺服端請求偽造

112年教育單位Top 10網站弱點



區網中心網站弱掃數量統計

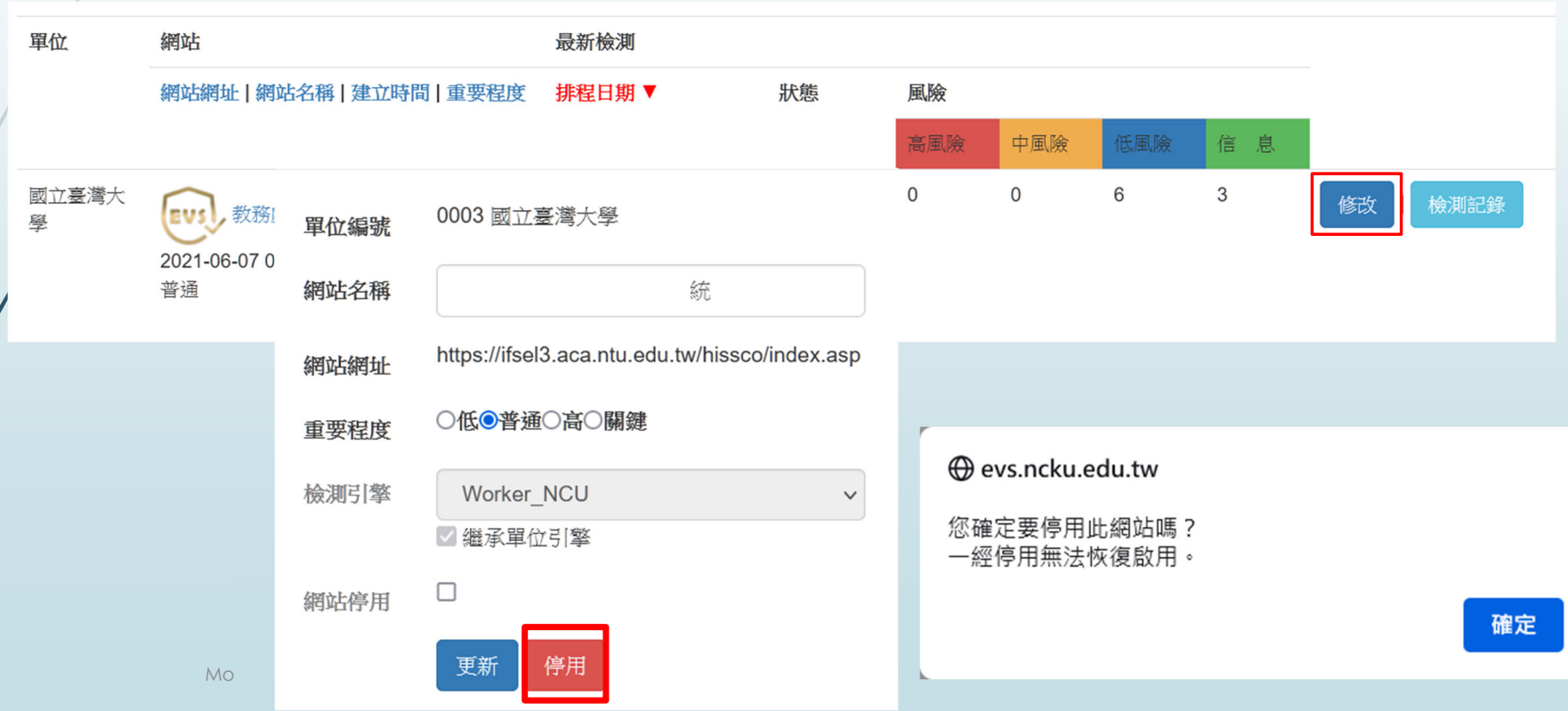
統計日期：112/05/15

年度	臺北I區	臺北II區	桃園區	竹苗區	新竹區	臺中區	南投區	雲嘉區	臺南區	高屏澎區	宜蘭區	花蓮區	臺東區	小計
108	278	159	35	374	98	142	30	265	163	508	22	26	30	2130
109	462	133	36	88	270	257	52	254	266	706	59	41	46	2670
110	341	151	15	50	128	97	33	199	240	391	61	20	15	1741
111	201	177	7	71	142	406	54	235	372	271	82	42	48	2108
112	61	104	2	21	21	136	27	143	95	239	30	17	13	909

單位：掃描次數

建議

- 務必針對中、**高風險網站**優先修補
- 已不服務的網站，請至EVS平台註記網站**已停用**



EVS平台注意事項

- 登入後需確認單位**資安責任等級**
- 申請弱掃網站應有**SSL憑證**
- 若為核心系統卻排不上弱掃**請提出核心系統證明，可協助排程**
- 新授權網站每日有**額度限制**
- 大量網站弱掃需求(一次須掃50個網站以上)，需提出申請

弱掃**前**注意事項

- 弱掃前，請備份網站，因弱掃可能造成資料遺失毀損等狀況。
- 請提前公告弱掃時間，提醒使用者該時段網站服務有可能會中斷。
- 請注意是否有其他資安設備，各資安設備、防火牆皆須開弱掃引擎白名單。
- 弱掃期間，建議關閉防毒軟體。
- 弱掃時間最長為**7**小時，若超過**7**小時系統會自動中斷掃描，因此建議先整理網站目錄，將不必要的檔案移除**(**例如備份檔**)** 。
- 因弱掃時會快速發送大量的請求(requests)，有可能造成網站服務中斷，或資安設備的異常狀況。除了提前公告弱掃時間外，建議**避免同單位多個網站都集中在同一時段弱掃。**

弱掃時機

- 網站公開上線前
- 職務異動新接系統
- 各區縣市往轄下被開立DEF事件單者
- B級單位網站每年建議執行一次
- C級單位網站每兩年建議執行一次
- 開發程式過程中

弱掃後常見異常狀況

- **掃描超過七小時**
  - 掃描時間過長，系統自動中斷掃描
  - 弱掃報告仍然有效，建議依報告修補弱點後，再進行複測
- **不論執行完成/失敗，只要掃描小於1分鐘，不會產生弱掃報告**
  - 可能原因：資安設備阻擋、該網址/IP未開啟Web服務、網路異常...
  - 建議排除上述原因後，重新申請排程掃描

系統弱點掃描軟體

- Nessus
- Openvas
- Nmap
- Microsoft Security Compliance Toolkit 1.0 (SCT)
- Microsoft Baseline Security Analyzer（MBSA）

宣導事項

宣導事項

- 如果有發生資安事件請自行通報。
- 通報要在**1小時**內完成。
- 若有病毒程式或檔案，建議**不要**放到公開網站上。如：VirusTotal

END